



Documento di ePolicy

RIMM035009

CPIA 6

VIA C. CESI 1 - 02100 - RIETI - RIETI (RI)

GERARDINA VOLPE

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del [Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente](#) e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

1. **Presentazione dell'ePolicy**
 1. Scopo dell'ePolicy
 2. Ruoli e responsabilità
 3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
 4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
 5. Gestione delle infrazioni alla ePolicy
 6. Integrazione dell'ePolicy con regolamenti esistenti
 7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curriculum**
 1. Curriculum sulle competenze digitali per gli studenti
 2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
 3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
 4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
 1. Protezione dei dati personali
 2. Accesso ad Internet
 3. Strumenti di comunicazione online
 4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
 1. Sensibilizzazione e prevenzione
 2. Cyberbullismo: che cos'è e come prevenirlo
 3. Hate speech: che cos'è e come prevenirlo
 4. Dipendenza da Internet e gioco online
 5. Sexting
 6. Adescamento online
 7. Pedopornografia
5. **Segnalazione e gestione dei casi**
 1. Cosa segnalare
 2. Come segnalare: quali strumenti e a chi
 3. Gli attori sul territorio per intervenire
 4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Il CPIA 6 Interprovinciale Rieti-Roma ha elaborato e adottato il presente documento e-policy nella consapevolezza dell'importanza di condividere con l'intera comunità scolastica principi e regole per un utilizzo consapevole e responsabile delle TIC e della Rete. In particolare, l'educazione alla cittadinanza digitale e alle buone pratiche sulla sicurezza in Rete e sull'utilizzo dei dispositivi digitali assume ancor più rilevanza, data la particolare utenza del CPIA, la cui azione educativa e formativa è rivolta prevalentemente a giovani e adulti, spesso con scarsa conoscenza nel campo dei dispositivi digitali.

Ai fini della redazione si è tenuto conto delle linee di orientamento emanate dal MIUR ad ottobre del 2017 per la prevenzione e il contrasto del cyberbullismo e delle indicazioni proposte dal progetto "Generazioni Connesse" realizzato su indicazioni del MIUR e della Commissione Europea con il supporto di: Polizia Postale, Garante per l'Infanzia e associazioni che operano in difesa dei diritti dei ragazzi.

1.2 - Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

Ai fini della promozione di un uso consapevole delle TIC, tenendo conto delle peculiarità della nostra scuola, la quale rivolge la sua azione formativa sia a giovani in età evolutiva che a individui adulti, per lo più stranieri e in cerca di occupazione, individua come attori principali le seguenti figure, ciascuna con il proprio ruolo e responsabilità:

Il **Dirigente scolastico**, è il garante della sicurezza anche online, di tutti i membri della comunità scolastica, pertanto è chiamato a gestire ed intervenire qualora si verificano casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali. Inoltre, il Dirigente Scolastico fornisce in collaborazione con il docente referente sulle tematiche del bullismo/cyberbullismo, il proprio contributo all'organizzazione di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC.

L'**Animatore Digitale**, supportato dal Team dell'Innovazione, promuove percorsi di formazione interna all'Istituto negli ambiti del Piano Nazionale Scuola Digitale, favorendo la partecipazione di tutta la comunità scolastica alle attività formative, allo scopo di realizzare una cultura digitale condivisa. Inoltre, l'Animatore Digitale cura l'aggiornamento del sito web della scuola e, sulla base dell'analisi dei fabbisogni della scuola, individua in sinergia con figure preposte all'assistenza tecnico-informatica, eventuali soluzioni metodologiche e tecnologiche utili da diffondere all'interno dell'Istituto.

Il **referente bullismo e cyberbullismo** coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tale scopo può avvalersi anche della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Il suo ruolo non si esaurisce all'interno della scuola in quanto coinvolge con progetti e percorsi formativi ad hoc, studenti, colleghi, genitori/tutori di studenti minorenni e associazioni del territorio che si occupano di stranieri e di migranti.

Il **Team per l'Innovazione Tecnologica supporta l'Animatore Digitale** e accompagna, adeguatamente, l'innovazione didattica nella scuola con il compito di favorire il processo di digitalizzazione nelle scuole, nonché quello di diffondere politiche legate all'innovazione didattica attraverso azioni di accompagnamento e di sostegno al Piano Nazionale per la Scuola Digitale sul territorio, nonché attraverso la creazione di gruppi di lavoro ed il coinvolgimento di tutto il personale della scuola.

La **Funzione Strumentale per la Gestione E Diffusione delle Nuove Tecnologie per la Scuola Digitale** supporta i docenti nell'utilizzo del Registro Elettronico, delle Piattaforme Elettroniche Ministeriali, e nell'utilizzo didattico delle nuove tecnologie informatiche e multimediali. Si occupa della gestione e diffusione del materiale didattico, fruibile attraverso le TIC, anche tramite il sito web dell'Istituto.

I **docenti**, in qualità di educatori, devono formarsi sulle tematiche riguardanti l'uso consapevole delle TIC e della Rete, in modo tale da diffondere tra gli studenti la cultura dell'uso responsabile di questi strumenti. In tal senso, essi presentano all'animatore digitale e al team dell'innovazione eventuali esigenze formative, segnalano eventuali problemi di carattere informatico e formulano proposte utili alla diffusione o all'aggiornamento delle buone pratiche in materia di gestione dei rischi nell'uso delle TIC e di internet. I docenti sono chiamati a promuovere l'applicazione delle tecnologie digitali nella didattica, integrando parti del curriculum della propria disciplina con opportuni approfondimenti. Essi supportano i propri studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, i docenti devono comunicare ai genitori/tutori degli alunni minorenni eventuali condotte non adeguate rilevate ad un uso scorretto delle TIC in modo da concordare opportune linee di intervento educative. Infine, i docenti hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il **personale Amministrativo Tecnico Ausiliario (ATA)** comprende una serie di figure che si occupano, in sinergia e ciascuna per la propria mansione, del funzionamento dell'Istituto scolastico per quanto concerne il settore amministrativo, contabile, gestionale e di sorveglianza. Il personale ATA deve essere consapevole dei problemi legati ad un uso scorretto delle TIC e della Rete per poterne fare uso in modo responsabile ed essere in grado di monitorare la corretta applicazione delle buone pratiche e segnalare eventuali abusi o irregolarità al Dirigente Scolastico. Inoltre, il personale ATA deve essere coinvolto in attività di formazione sul tema del bullismo e del cyberbullismo, nella segnalazione -insieme ad altre figure- di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Il **Direttore dei Servizi Generali e Amministrativi (DSGA)** garantisce, attraverso l'intervento di tecnici specializzati e nei limiti delle risorse finanziarie dell'Istituto, che l'apparato tecnico-informatico sia funzionante, sicuro e non esposto ad attacchi esterni o ad usi impropri. Inoltre, il Direttore dei Servizi Generali e Amministrativi garantisce che ci sia un adeguato funzionamento dei sistemi di comunicazione all'interno della scuola (es. circolari, sito web, ecc.) e tra scuola e genitori/tutori/associazioni per la notifica di documenti e informazioni attinenti l'uso delle TIC e della Rete.

Gli **Studenti** e le **Studentesse** devono saper utilizzare responsabilmente le tecnologie digitali, in coerenza con quanto richiesto dai docenti; conoscere i rischi della Rete, adottando condotte rispettose degli altri, imparando a tutelarsi online e a tutelare i/le propri/e compagni/e; promuovere le buone pratiche apprese all'interno della classe e della scuola e partecipare ad attività che favoriscano un uso positivo, critico e consapevole delle TIC e della Rete.

I **genitori/tutori** degli alunni minorenni sono invitati a condividere i principi educativi della scuola, anche in merito ad un utilizzo corretto e responsabile delle TIC e della Rete, relazionandosi in modo positivo e costruttivo con i docenti, mettendoli al corrente di eventuali problematiche relative a questi temi. In tal senso, è fondamentale che i genitori/tutori degli alunni minorenni accettino e condividano pienamente quanto scritto nella e-policy d'Istituto. È opportuno, inoltre, che siano partecipi attivamente ai progetti e alle attività messe in atto dalla scuola per sensibilizzare gli studenti e le studentesse ai rischi connessi ad un uso improprio delle tecnologie digitali, a partire da quello dei device personali (es. smartphone);

Gli **Enti educativi esterni e le Associazioni** devono conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della Rete e promuovere comportamenti sicuri, la sicurezza online, assicurando la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Quanti saranno chiamati ad interagire, a vario titolo, con l'Istituto per la realizzazione di attività educative o progetti dovranno tenere conto della e-Policy dell'Istituto, rispettando le disposizioni in essa contenute.

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;

- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

La ePolicy è un documento condiviso da tutti gli attori appartenenti alla comunità scolastica:

Gli ALUNNI dovranno essere informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno utilizzati sotto il controllo degli insegnanti dopo essere stati istruiti riguardo all'uso responsabile e sicuro di Internet e della rete. L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule con accesso a Internet e sul sito della scuola.

I DOCENTI sono tenuti ad informare gli alunni del regolamento per l'uso della rete scolastica. Gli organi collegiali stabiliranno la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sarà comunicata formalmente a tutto il personale con il presente documento e diffusa sul sito web della scuola. Il personale docente dovrà avere un'adeguata informazione/formazione nell'uso sicuro e responsabile di Internet.

I GENITORI nel caso di studenti minorenni saranno informati, all'atto dell'iscrizione del regolamento, dell'uso delle TIC attraverso anche il sito web della scuola.

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Le potenziali infrazioni in cui è possibile che gli alunni incorrano nell'utilizzo delle TIC di cui si dispone per la didattica, possono essere: l'uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare; l'invio incauto o senza permesso di foto e dati personali; la comunicazione incauta e senza permesso con

sconosciuti; il collegamento a siti web non idonei.

Nel caso di cattivo uso saranno previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni. Se ciò non risultasse sufficiente saranno presi provvedimenti disciplinari.

Per il personale scolastico, in particolare per i docenti, le possibili infrazioni in cui incorrere sono un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non conforme alle attività di insegnamento o al profilo professionale; un utilizzo delle e-mail con gli alunni e i genitori/tutor (in caso di minori) non compatibile con il ruolo professionale; un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy. Le procedure di controllo sono quelle previste dalla legge e dai contratti di lavoro.

In caso di alunni minorenni i genitori dovrebbero tenere condotte atte a favorire l'uso corretto delle TIC, auspicando un controllo nella navigazione sul web. I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, qualora dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Tutti gli attori coinvolti vengono informati della pubblicazione del presente "Regolamento per l'uso delle risorse tecnologiche e di rete" della scuola e possono prenderne visione sul sito istituzionale della scuola.

1.7 - Monitoraggio

dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il Dirigente Scolastico in collaborazione con l'Animatore Digitale , il Team per l'Innovazione, Funzione Strumentale per la Gestione E Diffusione delle Nuove Tecnologie per la Scuola Digitale e il Referente del Bullismo e del Cyberbullismo si occupa di monitorare l'implementazione della e-Policy e di rilevare la eventuale necessità di un aggiornamento della stessa.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare un gruppo di lavoro per la stesura del documento di e-Policy
- Informare la comunità scolastica sui contenuti del documento di e-Policy

Azioni da svolgere nei prossimi 3 anni:

- Informare la comunità scolastica sull'eventuale aggiornamento del documento di e-Policy

Capitolo 2 - Formazione e curriculum

2.1. Curriculum sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”.

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” ([“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

Le persone dovrebbero comprendere in che modo le tecnologie digitali possono essere di aiuto alla comunicazione, alla creatività e all’innovazione, pur nella consapevolezza di quanto ne consegue in termini di opportunità, limiti, effetti e rischi. Dovrebbero comprendere i principi generali, i meccanismi e la logica che sottendono alle tecnologie digitali in evoluzione, oltre a conoscere il funzionamento e l’utilizzo di base di diversi dispositivi, software e reti. Dovrebbero assumere un approccio critico nei confronti della validità, dell’affidabilità e dell’impatto delle informazioni e dei dati resi disponibili con strumenti digitali ed essere consapevoli dei principi etici e legali chiamati in causa con l’utilizzo delle tecnologie digitali.

Tutti dovrebbero essere in grado di utilizzare le tecnologie digitali come ausilio per la cittadinanza attiva e l’inclusione sociale, la collaborazione con gli altri e la creatività nel raggiungimento di obiettivi personali, sociali o commerciali. Le abilità comprendono la capacità di utilizzare, accedere, filtrare, valutare, creare,

programmare e condividere contenuti digitali. Le persone dovrebbero essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali, oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi. Interagire con tecnologie e contenuti digitali presuppone un atteggiamento riflessivo e critico, ma anche improntato alla curiosità, aperto e interessato al futuro della loro evoluzione. Impone anche un approccio etico, sicuro e responsabile all'utilizzo di tali strumenti." (["Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente"](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

Per progettare ed implementare un curriculum digitale, l'Istituzione scolastica prevede di intervenire su tutte le classi di I livello, I e II periodo didattico e nelle classi di alfabetizzazione da realizzarsi in prospettiva di continuità e trasversalità con le discipline del curriculum scolastico.

L'intervento nelle classi terrà conto delle dimensioni cui si riferiscono le "competenze digitali":

- dimensione tecnologica: fondamentale far riflettere i nostri studenti sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, supportandoli nella comprensione della "grammatica" dello strumento al fine di evitare automatismi;
- dimensione cognitiva: si riferisce alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;
- dimensione etica: farà riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili;
- dimensione sociale: pone l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative.

Nell'ambito del percorso formativo saranno affrontate alcune delle tematiche centrali per lo sviluppo delle competenze digitali: i diritti della rete, a partire dalla Dichiarazione per i Diritti in Internet redatta dalla Commissione per i diritti e i doveri relativi ad Internet della Camera dei Deputati; l'educazione ai media e alle dinamiche sociali online (social network); la qualità, integrità e circolazione dell'informazione (attendibilità delle fonti, diritti e doveri nella circolazione delle opere creative, privacy e protezione dei dati, information literacy).

Per definire le competenze digitali la scuola fa riferimento al DigComp che è diventato un modello per lo sviluppo e la pianificazione strategica di iniziative sulle competenze digitali.

Il DigComp ha individuato 21 competenze digitali, suddivise in 5 aree:

Area delle competenze 1: Alfabetizzazione su informazioni e dati

1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali

1.2 Valutare dati, informazioni e contenuti digitali

1.3 Gestire dati, informazioni e contenuti digitali

Area delle competenze 2: Comunicazione e collaborazione

2.1 Interagire con gli altri attraverso le tecnologie digitali

2.2 Condividere informazioni attraverso le tecnologie digitali

2.3 Esercitare la cittadinanza attraverso le tecnologie digitali

2.4 Collaborare attraverso le tecnologie digitali

2.5 Netiquette

2.6 Gestire l'identità digitale

Area delle competenze 3: Creazione di contenuti digitali

3.1 Sviluppare contenuti digitali

3.2 Integrare e rielaborare contenuti digitali

3.3 Copyright e licenze

3.4 Programmazione

Area delle competenze 4: Sicurezza

4.1 Proteggere i dispositivi

4.2 Proteggere i dati personali e la privacy

4.3 Proteggere la salute e il benessere

4.4 Protecting the environment

Area delle competenze 5: Risolvere problemi

5.1 Risolvere problemi tecnici

5.2 Individuare fabbisogni e risposte tecnologiche

5.3 Utilizzare in modo creativo le tecnologie digitali

5.4 Individuare i divari di competenze digitali

Per ciascuna delle 21 competenze sono stati individuati 8 livelli di padronanza, suddivisi in base, intermedio, avanzato, altamente specializzato (due livelli per ognuno di questi descrittori). Ciascun livello rappresenta un gradino in più nell'acquisizione da parte dei cittadini delle competenze in base alla sfida cognitiva, alla complessità delle attività che possono gestire e alla loro autonomia nello svolgimento dell'attività. Ogni livello è descritto attraverso esempi pratici.

Come per le altre competenze del percorso formativo, si cercherà di progettare un percorso ad hoc per ogni studente. La programmazione degli obiettivi si baserà sulle competenze, i livelli e le esemplificazioni previsti dal DigComp.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

La visione di Educazione nell'era digitale è il cuore del Piano Nazionale Scuola Digitale: un percorso condiviso di innovazione culturale, organizzativa, sociale e istituzionale che vuole dare nuova energia, nuove connessioni, nuove capacità alla scuola italiana. In questa visione, il "digitale" è strumento abilitante, connettore e volano di cambiamento. (PNSD, pag. 26)

Il personale della scuola deve essere equipaggiato per tutti i cambiamenti richiesti dalla modernità, e deve essere messo nelle condizioni di vivere e non subire l'innovazione. La formazione dei docenti sarà centrata sull'innovazione didattica,

tenendo conto delle tecnologie digitali come sostegno per la realizzazione dei nuovi paradigmi educativi e la progettazione operativa di attività. (PNSD, pag. 31)

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento.

Un utilizzo strutturato e integrato delle TIC nella didattica non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

I ragazzi nella comunicazione digitale esprimono se stessi, sviluppano la propria identità personale e sociale.

I dispositivi tecnologici, sempre presenti nella vita quotidiana, consentono loro di poter entrare in contatto con il mondo che li circonda.

Formare i docenti sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media ma anche considerare la sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie.

In quest'ottica è necessario avviare un percorso di formazione che abbracci, in un arco di tempo pluriennale, momenti di formazione differenti ma complementari.

I momenti di formazione e aggiornamento saranno pensati e creati partendo dall'analisi del fabbisogno formativo dei docenti sull'utilizzo e l'integrazione delle TIC

nella didattica; dall'analisi del fabbisogno conoscitivo circa particolari argomenti prioritari per i docenti e il CPIA; dall'analisi delle richieste che provengono dagli studenti e dalle studentesse in modo, poi, da riutilizzarli nel lavoro di insegnanti.

I docenti per tale motivo hanno necessità di seguire un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a queste ultime. Promuovere la formazione dei docenti sull'uso responsabile e sicuro della Rete e dei rischi ad essa collegati, richiede l'elaborazione di un cronoprogramma che consideri il triennio scolastico in una prospettiva di vera e propria programmazione per la formazione, con azioni specifiche quali:

- analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete con la somministrazione di un questionario;
- promuovere l'informazione e la promozione della partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
- monitorare in itinere le azioni svolte attraverso un sondaggio online;
- organizzare incontri con professionisti della scuola e con esperti esterni, enti/associazioni coinvolgendo le famiglie, gli studenti/le studentesse;
- creare un'area specifica nel sito della scuola con materiali formativi per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, facendo riferimento anche al link del progetto "Generazioni connesse".

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Per rinforzare l'alleanza educativa fra scuola, famiglie/tutor dei minori, e adulti che frequentano il nostro CPIA è necessario condividere percorsi sull'educazione digitale per una maggiore sensibilizzazione sulle tematiche relative alle TIC.

Importante è informare i genitori/tutor e adulti sui comportamenti da adottare a scuola elaborando regole sull'uso delle tecnologie digitali per le comunicazioni con la scuola e con i docenti (es. email, gruppo whatsapp, sito della scuola etc.); prevedendo azioni e strategie per il coinvolgimento delle famiglie in percorsi di sensibilizzazione, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.

Ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno. A tale proposito è importante informare i genitori/tutor sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli.

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica e per la comunità educante tutta. Si legge nelle Linee di indirizzo del MIUR il "Patto di Corresponsabilità educativa", punta a "rafforzare il rapporto scuola/famiglia in quanto nasce da una comune assunzione di responsabilità e impegna entrambe le componenti a dividerne i contenuti e a rispettarne gli impegni".

L'impegno del nostro Istituto è quello di aggiornare e integrare, oltre che il regolamento scolastico, anche il "Patto di corresponsabilità", con specifici riferimenti alle tecnologie digitali.

Ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Per tale motivo avvieremo un piano di azioni che si svilupperanno in un'annualità e in un arco di tre anni.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 - Protezione dei dati personali

“Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino”.

(cfr. <http://www.garanteprivacy.it/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il “corretto trattamento dei dati personali” a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

La scuola ha il dovere di tutelare la privacy dei discenti e delle loro famiglie, ma anche il compito di informarli e soprattutto renderli consapevoli di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri; pertanto, il nostro Cpia avrà cura di tutelare la privacy di tutti i propri corsisti: ricordiamo che tra la sua utenza di allievi si annoverano anche ristretti della Casa Circondariale, dunque è d'obbligo tutelare anche la privacy delle persone in relazione alla loro situazione interpersonale giudiziaria e luogo di residenza temporaneo.

La scuola informerà tutti gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento.

Come primo step la scuola individuerà gli addetti alla gestione della privacy e i referenti preposti alle diverse procedure, distinguendo i soggetti che trattano dati personali da coloro i quali non sono autorizzati ad accedervi.

In secondo luogo si procederà alla gestione efficiente del registro.

Come previsto dal Regolamento Ue 679/2016, il nostro Istituto si impegna a:

- designare la figura preposta alla protezione dei dati personali
- Redigere e mantenere un registro dei trattamenti dei dati, sia per il titolare che per il responsabile dei trattamenti.
- Valutare dei rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente alle diverse tipologie di trattamento dei dati sensibili.
- Effettuare analisi di processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara (art. 7.2).
- Adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti.
- Analizzare il sito web istituzionale di riferimento e, qualora fosse necessario, apportare modifiche che migliorino la sicurezza e la protezione dei dati trattati.
- Valutare proposte di messa in sicurezza della rete intranet scolastica.
- Rendere noto alle famiglie e agli alunni, quali dati vengono raccolti e come vengono utilizzati, secondo la normativa vigente, in materia di protezione dei dati personali.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

Una delle principali peculiarità dell'organizzazione didattica dell'Istruzione per Adulti è la Fruizione a Distanza (FAD), che si realizza proprio attraverso l'utilizzo delle ICT e che permette di sviluppare le competenze digitali degli studenti, favorire la personalizzazione dei percorsi ed offrire una concreta opportunità per la flessibilità

nella frequenza; l'emergenza pandemica, poi, ha introdotto DAD e DDI.

Tenendo conto che i nostri corsisti, in quanto adulti, necessitano di approcci maggiormente individualizzati in relazione alle caratteristiche di ognuno di loro, il nostro Istituto si impegna a:

- offrire iniziative in presenza e a distanza per il recupero degli apprendimenti e delle altre situazioni di svantaggio determinate anche dalla recente emergenza sanitaria;
- educare la comunità dei discenti ad un uso consapevole e responsabile degli strumenti digitali e delle nuove tecnologie nel rispetto dei regolamenti dell'Istituto;
- incoraggiare l'utilizzo delle nuove tecnologie a supporto degli apprendimenti, proponendo azioni di formazione e aggiornamento del personale scolastico in tema di competenze digitali.

Come stabilito dal Piano Nazionale Scuola Digitale (PNSD), il nostro CPIA ha istituito la figura dell'animatore digitale nell'ambito del proprio organico docenti di ruolo; quest'ultimo potrà sviluppare la progettualità su tre ambiti: formazione interna, coinvolgimento della comunità scolastica, organizzazione di soluzioni innovative.

Con l'ePolicy il nostro Istituto si doterà di un regolamento sull'uso delle TIC che preveda una sezione dedicata all'uso di Internet, in cui gli studenti si impegnano a utilizzare la rete in maniera corretta e consapevole e nel rispetto del Regolamento d'Istituto e delle indicazioni dei docenti.

I docenti si impegnano a formare gli studenti ad un uso corretto e consapevole della rete e a monitorare l'uso che gli stessi fanno delle tecnologie a scuola.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Gli strumenti di comunicazione online, attraverso l'interattività del mezzo, ci

permettono di superare le barriere spazio-temporali e promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo. Fra i vari strumenti di comunicazione, il nostro CPIA utilizza il Registro Elettronico, che consente la visualizzazione di molte informazioni utili ai corsisti e alle famiglie degli studenti minorenni, tra cui:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari, documenti di valutazione);
- lettura di circolari
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

Il Registro Elettronico è collegato ad una piattaforma esterna, utilizzata per la didattica a distanza: essa permette agli allievi di connettersi da remoto e di assistere a videolezioni di ogni disciplina, oltre all'inserimento di compiti a distanza multimediali (video, foto, articoli per il sito, documenti, elaborati anche di gruppo).

Oltre al Registro Elettronico, un fondamentale canale di comunicazione online è il sito istituzionale (raggiungibile all'indirizzo <https://www.cpiarieti.edu.it/>), costantemente aggiornato con avvisi, circolari ed eventi in evidenza: nel sito sono facilmente reperibili i contatti del Dirigente Scolastico, della segreteria, dei referenti di plesso.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente **ePolicy** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Il nostro CPIA, al fine di garantire una didattica digitale innovativa e sicura, si è dotato

di strumenti digitali presso tutte le proprie Sedi (LIM, tablet, computer, monitor multimediali), per consentire ai propri corsisti una lezione più interattiva e partecipata. Il Titolare del trattamento dei dati è il CPIA 6, nella persona del Dirigente Scolastico.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

Scegliere almeno 1 di queste azioni:

Organizzare un evento o attività volti a formare il personale dell'Istituto sul tema della protezione dei dati personali

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**.

- Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

I rischi online rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di ragazzi e ragazze: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia, pedopornografia, gioco d'azzardo o gambling, internet addiction, videogiochi online, esposizione a contenuti dannosi o inadeguati. Partendo da questo

punto di vista, vanno promosse nei più giovani le necessarie competenze e capacità, al fine di una protezione adeguata, ma anche al fine di un utilizzo consapevole che sappia sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni.

Il concetto di prevenzione per ciò che riguarda la sicurezza in Internet si risolve in una serie di interventi atti a promuovere competenze digitali consapevoli e quindi prive di rischi.

Il nostro CPIA metterà in campo tutte le strategie a sua disposizione o ne creerà delle altre, ove possibile, al fine di promuovere le competenze digitali e ridurre i rischi per la sicurezza di ragazze/i.

Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, appare chiaro dunque come le migliori strategie di intervento siano di carattere prevalentemente preventivo per consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online.

Le dimensioni che il fenomeno coinvolge sono molteplici e si rifanno soprattutto alle capacità dei giovani di gestire situazioni complesse che richiedono:

capacità di gestire relazioni con l'altro diverso da sé;

capacità di gestire le dimensioni dell'affettività e della sessualità;

il riconoscimento di un limite, anche, ma non solo, correlato ad una dimensione di legalità;

l'utilizzo sicuro e consapevole delle tecnologie digitali.

Per questo motivo la scuola deve rafforzare la sua capacità di risposta attraverso strumenti e misure specifiche e nel caso si verifichi un evento problematico connesso ai rischi online deve essere pronta a dare una risposta il più possibile immediata, chiara e che possa prevedere la collaborazione (mediante accordi specifici) con la rete dei servizi locali come ASL e Polizia Postale.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

“qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d’identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo”.

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di [cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
 - Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
 - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d’istituto), atti e documenti (PTOF, PdM, Rav).

Un’altra

indicazione operativa concerne una valutazione circa l’eventuale stato di disagio nel quale possa venirsi a trovare lo studente che potrebbe quindi avere bisogno di un supporto psicologico. In tal caso le strutture a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza.

Per quanto riguarda la necessità di segnalazione e rimozione, ciascun minore ultraquattordicenne, i suoi genitori o chi esercita la responsabilità del minore che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un’istanza per l’oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l’interessato può rivolgere analoga richiesta al Garante per la protezione dei dati

personali, che rimuoverà i contenuti entro 48 ore. Il Garante ha pubblicato nel proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gdpd.it.

Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato come: il furto di identità o la persistenza di una condotta persecutoria che metta seriamente a rischio il benessere psicofisico della vittima, si potrà inoltrare una denuncia/querela agli uffici preposti delle Forze di Polizia e permettere così alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo.

Gli uffici preposti a tal scopo sono: Polizia di Stato - Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri - Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato - Commissariato on line (attraverso il portale <http://www.commissariatodips.it>).

Per un consiglio e un supporto è possibile rivolgersi alla Helpline di Telefono Azzurro per Generazioni Connesse: operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei media digitali.

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media

digitali e i social network;

- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Il nostro CPIA nell'ambito dell'educazione civica affronterà i seguenti temi:

- il discorso dell'odio online
- diritti umani
- la libertà di espressione
- il razzismo e la discriminazione
- vita privata e sicurezza
- democrazia e partecipazione

La mission del CPIA così come indicato nel PTOF è finalizzata prioritariamente all'educazione e all'istruzione delle persone con bisogni specifici. Proprio per questo la nostra Istituzione scolastica pone costantemente al centro della propria azione tematiche come l'integrazione e la lotta ad ogni forma di discriminazione.

Il nostro CPIA organizzerà corsi di alfabetizzazione digitale per evitare che i giovani riproducano alcuni aspetti negativi e certe cattive abitudini che inducono al fenomeno dell'odio online.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

La Società Italiana Intervento Patologie Compulsive definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza, mentre la nomofobia si caratterizza come la necessità compulsiva di rimanere connessi col proprio smartphone.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della

tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D), sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, se affrontiamo il problema della dipendenza dal gioco, ci sono chiari segnali nel comportamento del giocatore che devono indurre in allarme.

La gestione e la cura di questa vera e propria patologia che coinvolge fattori bio-socio-psicologici richiede un intervento serio e competente da parte di figure professionali altamente specializzate. Tuttavia, nella fase iniziale, la scuola può contribuire alla rilevazione di un problema di dipendenza attraverso un'attenta osservazione di alcuni comportamenti distorti che possono indurre a ipotizzare l'esistenza di una anomalia, come la progressiva riduzione dei contatti sociali, manifestazioni di ansia o rabbia per l'impossibilità di rimanere connessi alla rete, atteggiamenti ossessivi.

Se in questa fase la scuola può svolgere una preziosa azione di monitoraggio e di raccordo con le famiglie o con le figure tutoriali, per allertare l'attenzione e innescare un intervento tempestivo, affidando poi agli esperti la risoluzione di un problema che non può certo rientrare nel suo raggio di competenza, tuttavia essa può mettere in atto interventi per la prevenzione e la sensibilizzazione nei confronti di questo fenomeno.

La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale all'apprendimento. Gli stessi videogiochi se utilizzati correttamente, possono rappresentare una risorsa didattica. Si potrebbe riflettere per stimolare la consapevolezza su tutte quelle attività che vengono compiute quotidianamente spesso in modo meccanico: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potrei cambiare quando sono online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella mia vita?

Azioni da svolgere nei confronti degli alunni:

- Incoraggiare e assegnare attività on-line di alta qualità come ricercare informazioni scientifiche, ricercare e promuovere corrispondenza con studenti nel mondo
 - Proporsi come destinatari di ascolto delle problematiche degli studenti
 - Fornire regole chiare sull'utilizzo del cellulare in classe e sulle conseguenze derivanti dal mancato rispetto di tali regole, che vanno comunicate all'inizio dell'anno scolastico all'interno del patto di corresponsabilità
 - Il cellulare deve configurarsi unicamente come strumento integrativo per la didattica sotto la guida del docente. Qualsiasi altro utilizzo non è previsto in quanto la classe è un ambiente di apprendimento con procedure e tempi dedicati che non prevedono sovrapposizioni e commistioni con un diverso uso dei device.
-

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti medialmente sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini o video sessualmente espliciti". I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/negli altri e depressione.

E' auspicabile che il CPIA organizzi periodicamente degli incontri con psicologi, esperti del diritto (magistrati, avvocati penalisti) aperti ai genitori dei corsisti minorenni, al fine di mettere in guardia gli allievi sui rischi penali a cui vanno incontro nella diffusione di immagini dal contenuto sessualmente esplicito. Ciò al fine di evitare che sull'alunno possa gravare un procedimento penale per diffusione anche inconsapevole di materiale pedopornografico.

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di

instant messaging (whatsapp, telegram etc.), i siti e le app di **teen dating** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies - l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori/tutori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui tali temi.

Fondamentale quindi, come sappiamo, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...), e nel caso in cui sorgessero significative problematiche psicologiche, potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *“Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”*, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n. 38 del 6 febbraio 2006** *“Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest’ultima, introduce, tra le altre cose, il reato di “pornografia minorile virtuale” (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un’ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d’età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un’attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **“Segnala contenuti illegali” (Hotline)**.

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il “Clicca e Segnala” di [Telefono Azzurro](#) e “STOP-IT” di [Save the Children](#).

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Inoltre in caso di rischio per il benessere psicofisico dei ragazzi/e coinvolte nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria, centri specializzati sull'abuso e il maltrattamento dei giovani e degli adolescenti, etc.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento a: Polizia di Stato - Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato - Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri - Comando Provinciale o Stazione del territorio di competenza. I più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo, come già sottolineato, l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

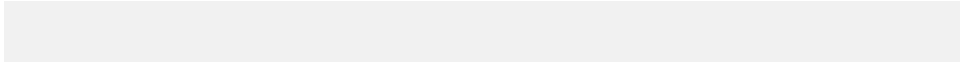
Scegliere almeno 1 di queste azioni:

- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.



Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.**
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenni e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per

segnalare la presenza di materiale pedopornografico online.

Saranno oggetto di segnalazione tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei Social Network. In particolare:

- contenuti afferenti la violazione della privacy;
 - contenuti afferenti all' aggressività o alla violenza;
 - contenuti afferenti alla sessualità.
-

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) - Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) - Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;

- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

Strumenti di segnalazione messi a disposizione degli studenti dal CPIA 6:

- e-mail del Dirigente Scolastico (ds.gerardinavolpe@cpiarieti.com);
- tutti i docenti dell'Istituto;
- un indirizzo e-mail specifico per le segnalazioni (di prossima attivazione);
- scatola/box per la raccolta di segnalazioni anonime.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di

governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

Il territorio di riferimento prevede agenti e strutture comuni ad altre realtà locali. Nella fattispecie si segnalano:

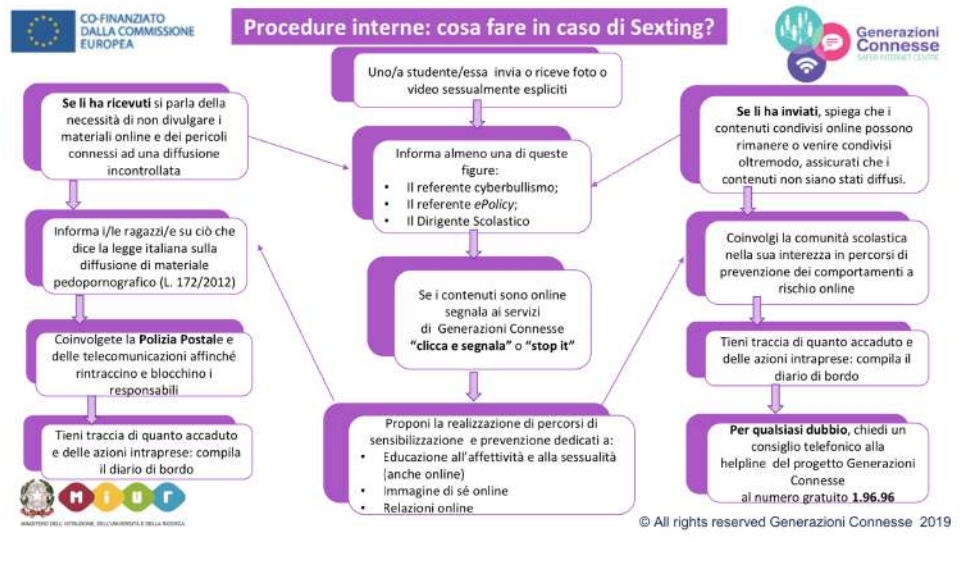
- il Comune;
 - le Comunità di accoglienza per i migranti;
 - le Case Famiglia;
 - le Forze dell'Ordine;
 - le Associazioni presenti sul territorio.
-

5.4. - Allegati con le procedure

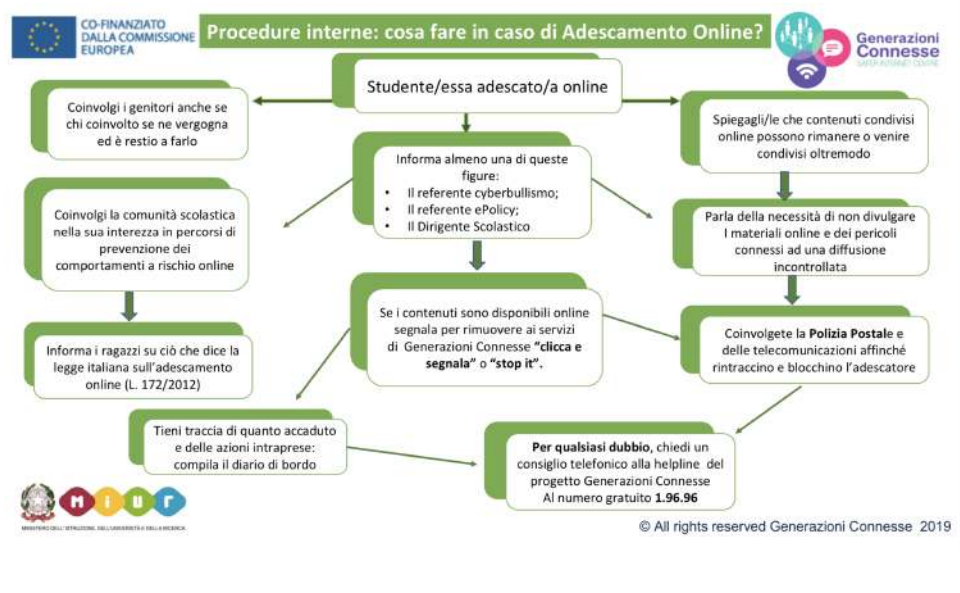
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



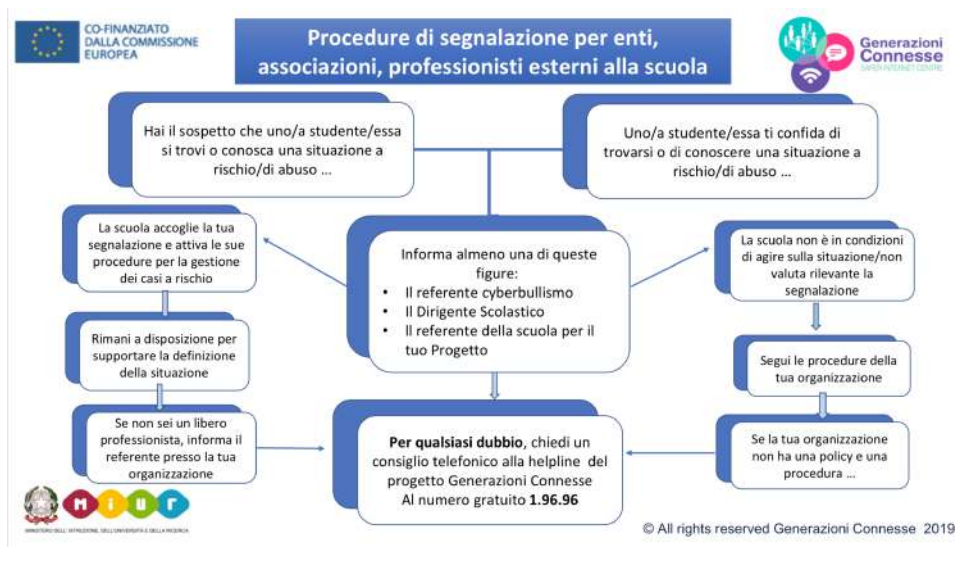
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

- [Scheda di segnalazione](#)
- [Diario di bordo](#)
- [iGloss@ 1.0 l'ABC dei comportamenti devianti online](#)
- [Elenco reati procedibili d'ufficio](#)

Il nostro piano d'azioni

Non è prevista nessuna azione.

